

# UNIQUENESS OF CERTAIN COMPLETELY REGULAR HADAMARD CODES

NEIL I. GILLESPIE AND CHERYL E. PRAEGER

ABSTRACT. We classify binary completely regular codes of length  $m$  with minimum distance  $\delta$  for  $(m, \delta) = (12, 6)$  and  $(11, 5)$ . We prove that such codes are unique up to equivalence, and in particular, are equivalent to certain Hadamard codes. Moreover, we prove that these codes are completely transitive.

## 1. INTRODUCTION

In 1973 Delsarte [9] introduced a class of codes with a high degree of combinatorial symmetry called *completely regular codes* (see Definition 2.1). Examples of such codes include the Hamming, Golay, Preparata, and Kasami codes. However, a belief began to emerge amongst coding theorists that completely regular codes with good error correcting capabilities are rare [18]. Indeed, in 1992, Neumaier [19] conjectured that the only completely regular code containing more than two codewords with minimum distance at least 8 is the extended binary Golay code. Despite this, there has been renewed interest in the subject. Borges, Rifà and Zinoviev have written a series of papers classifying various families and finding new examples of completely regular codes [3, 20, 21, 24], and in particular, they give a counter example to Neumaier's conjecture [2]. Moreover, they also show that many of these examples are *completely transitive* (see Definition 2.1), a subclass of completely regular codes. Given these new discoveries, we consider the following two problems posed by Neumaier in his 1992 paper.

- Find all 'small' completely regular codes in Hamming graphs.
- Characterise the known completely regular codes by their parameters.

In relation to these two questions we draw attention to two beautiful examples of binary completely regular codes; *the Hadamard 12 code* and *the punctured Hadamard 12 code* (see Section 4). In this paper we characterise these codes by their parameters and prove the following.

**Theorem 1.1.** *Let  $C$  be a binary completely regular code of length  $m$  with minimum distance  $\delta$ .*

- (a) *If  $m = 12$  and  $\delta = 6$ , then  $C$  is equivalent to the Hadamard 12 code;*
- (b) *If  $m = 11$  and  $\delta = 5$ , then  $C$  is equivalent to the punctured Hadamard 12 code.*

---

This paper is dedicated to Kathryn Horadam in honour of her 60th birthday.

Date: draft typeset October 30, 2012

2000 Mathematics Subject Classification: 05C25, 20B25, 94B05.

Key words and phrases: *completely regular codes, completely transitive codes, Hadamard codes, Mathieu groups.*

This research was supported by the Australian Research Council Federation Fellowship FF0776186 of the second author, and for the first author, by an Australian Postgraduate Award.

Moreover the codes  $C$  in (a) and (b) are completely transitive.

In Section 2, we introduce our notation and preliminary results. The Hadamard 12 code is an example of a *Hadamard code*, a family of codes generated by Hadamard matrices, which we describe in Section 3, and prove that the automorphism group of a matrix is isomorphic to the automorphism group of the code it generates. In the subsequent section we prove that the Hadamard 12 and punctured Hadamard 12 codes are completely transitive. In the final section we prove Theorem 1.1.

## 2. DEFINITIONS AND PRELIMINARIES

Any binary code of length  $m$  can be embedded as a subset of the vertex set of the binary Hamming graph  $\Gamma = H(m, 2)$ , which has a vertex set  $V(\Gamma)$  that consists of  $m$ -tuples with entries from the field  $\mathbb{F}_2 = \{0, 1\}$ , and an edge exists between two vertices if and only if they differ in precisely one entry. The automorphism group of  $H(m, 2)$ , which we denote by  $\text{Aut}(\Gamma)$ , is the semi-direct product  $B \rtimes L$  where  $B \cong S_2^m$  and  $L \cong S_m$  [6, Thm. 9.2.1]. Let  $g = (g_1, \dots, g_m) \in B$ ,  $\sigma \in L$  and  $\alpha = (\alpha_1, \dots, \alpha_m) \in V(\Gamma)$ . Then  $g\sigma$  acts on  $\alpha$  in the following way:

$$\alpha^{g\sigma} = (\alpha_{1\sigma^{-1}}^{g_1^{\sigma^{-1}}}, \dots, \alpha_{m\sigma^{-1}}^{g_m^{\sigma^{-1}}}).$$

Let  $M = \{1, \dots, m\}$ . The *support* of  $\alpha$  is the set  $\text{supp}(\alpha) = \{i \in M : \alpha_i \neq 0\}$ , and the *weight* of  $\alpha$  is the size of the set  $\text{supp}(\alpha)$ . For all pairs of vertices  $\alpha, \beta \in V(\Gamma)$ , the *Hamming distance* between  $\alpha$  and  $\beta$ , denoted by  $d(\alpha, \beta)$ , is defined to be the number of entries in which the two vertices differ. We let  $\Gamma_k(\alpha)$  denote the set of vertices in  $\Gamma$  that are at distance  $k$  from  $\alpha$ .

A code  $C$  in  $H(m, 2)$  is an  $(m, N, \delta)$  code if  $N = |C|$ , the number of codewords of  $C$ , and  $\delta$  is the *minimum distance* of  $C$ , the smallest distance between distinct codewords of  $C$ . For any vertex  $\gamma \in V(\Gamma)$ , we define the *distance of  $\gamma$  from  $C$*  to be  $d(\gamma, C) = \min\{d(\gamma, \beta) : \beta \in C\}$ . The *covering radius*  $\rho$  of  $C$  is the maximum distance any vertex in  $H(m, 2)$  is from  $C$ . We let  $C_i$  denote the set of vertices that are distance  $i$  from  $C$ . It follows that  $\{C = C_0, C_1, \dots, C_\rho\}$  forms a partition of  $V(\Gamma)$ , called the *distance partition of  $C$* . Let  $C'$  be another code in  $H(m, 2)$ . We say  $C$  and  $C'$  are *equivalent* if there exists  $x \in \text{Aut}(\Gamma)$  such that  $C^x = C'$ , and if  $C = C'$ , we call  $x$  an *automorphism of  $C$* . The *automorphism group of  $C$*  is the setwise stabiliser of  $C$  in  $\text{Aut}(\Gamma)$ , which we denote by  $\text{Aut}(C)$ . The *distance distribution of  $C$*  is the  $(m+1)$ -tuple  $a(C) = (a_0, \dots, a_m)$  where

$$(2.1) \quad a_i = \frac{|\{(\alpha, \beta) \in C^2 : d(\alpha, \beta) = i\}|}{|C|}.$$

We observe that  $a_i \geq 0$  for all  $i$  and  $a_0 = 1$ . Moreover,  $a_i = 0$  for  $1 \leq i \leq \delta - 1$  and  $|C| = \sum_{i=0}^m a_i$ . The *MacWilliams transform* of  $a(C)$  is the  $(m+1)$ -tuple  $a'(C) = (a'_0, \dots, a'_m)$  where

$$(2.2) \quad a'_k := \sum_{i=0}^m a_i K_k(i)$$

with

$$K_k(x) := \sum_{j=0}^k (-1)^j \binom{x}{j} \binom{m-x}{k-j}.$$

It follows from [16, Lem. 5.3.3] that  $a'_k \geq 0$  for  $k = 0, 1, \dots, m$ . We say  $C$  has *external distance*  $s$  if there are exactly  $s + 1$  nonzero entries in  $a'(C)$ .

**Definition 2.1.** Let  $C$  be code with distance partition  $\{C = C_0, C_1, \dots, C_\rho\}$  and  $\gamma \in C_i$ . We say  $C$  is *completely regular* if  $|\Gamma_k(\gamma) \cap C|$  depends only on  $i$  and  $k$ , and not on the choice of  $\gamma \in C_i$ . If there exists  $G \leq \text{Aut}(\Gamma)$  such that each  $C_i$  is a  $G$ -orbit, then we say  $C$  is  *$G$ -completely transitive*, or simply *completely transitive*.

A narrower definition of complete transitivity for binary linear codes was first introduced by Solé [22]. Giudici and the second author [12] extended Solé's definition to cover linear codes over any finite field, referring to such codes as *coset-completely transitive*. (This is the definition used by Borges et al. in their series of papers.) In the same paper, Giudici and the second author further generalised this concept. (The definition given here is the one given in [12], but in the binary case.) They proved that coset-completely transitive codes are necessarily completely transitive, and that completely transitive codes are completely regular. Moreover, they showed that the repetition code of length 3, over an alphabet with large enough cardinality, is completely transitive but not coset-completely transitive. We give two additional examples in this paper (Proposition 4.1 and 4.2), which are binary and non-trivial. The following result is straight forward, but useful in Section 4 where we prove the complete transitivity of these examples.

**Lemma 2.2.** *Let  $C$  be a code in  $H(m, 2)$  such that  $\text{Aut}(C)$  acts transitively on  $C$ . If  $\text{Aut}(C)_\alpha$  acts transitively on  $\Gamma_i(\alpha) \cap C_i$  for some  $\alpha \in C$ , then  $\text{Aut}(C)$  acts transitively on  $C_i$ .*

A code  $C$  with covering radius  $\rho$  and minimum distance  $\delta$  is *uniformly packed (in the wide sense)*, if there exist rational numbers  $\lambda_0, \dots, \lambda_\rho$  such that  $\sum_{i=0}^\rho \lambda_i f_k(\nu) = 1$  for all vertices  $\nu$ , where  $f_k(\nu) = |\Gamma_k(\nu) \cap C|$ . The case  $\rho = e + 1$ , with  $e = \lfloor \frac{\delta-1}{2} \rfloor$ , corresponds to the *uniformly packed codes* defined by Goethals and van Tilborg [13]. For any code  $C$  of length  $m$ , the *extended code*  $C^*$  of length  $m + 1$  is generated by adding a parity check bit to each codeword of  $C$ . In the case that  $C$  is a binary uniformly packed code, Bassalygo and Zinoviev [1] gave necessary and sufficient conditions for  $C^*$  to be uniformly packed. The following result seems to be well known, but the authors could not find a proof in the literature, so we give a simple argument here.

**Lemma 2.3.** *Let  $C$  be a binary uniformly packed code with covering radius  $\rho = e + 1$ , where  $e = \lfloor \frac{\delta-1}{2} \rfloor$ , such that the extended code  $C^*$  is uniformly packed. Then  $C^*$  is completely regular.*

*Proof.* It is straight forward to deduce that  $C^*$  has minimum distance  $\delta^* = 2e + 2$ . Moreover, by [5],  $C^*$  has covering radius  $\rho^* = \rho + 1$ . As  $C^*$  is uniformly packed, it follows from [1] that it has external distance  $s^* = \rho^* = \rho + 1 = e + 2$ . Consequently,  $2s^* - 2 = 2e + 2 = \delta^*$ , and because  $C^*$  consists entirely of codewords of even weight, it follows from [6, p.347] that  $C^*$  is completely regular.  $\square$

For any  $\alpha \in V(\Gamma)$ , the *complement* of  $\alpha$  is the unique vertex  $\alpha^c$  with  $\text{supp}(\alpha^c) = M \setminus \text{supp}(\alpha)$ , and we say a code  $C$  is *antipodal* if  $\alpha^c \in C$  for all  $\alpha \in C$ .

Let  $p \in M = \{1, \dots, m\}$  and  $C$  be a code in  $H(m, 2)$ . By deleting the same coordinate  $p$  from each codeword of  $C$ , we generate a code  $C^{(p)}$  in  $H(m - 1, 2)$ , which we call the *punctured code of  $C$  with*

respect to  $p$ . We can also describe  $C^{(p)}$  in the following way. Let  $J = \{i_1, \dots, i_k\} \subseteq M$  and define the following map

$$\begin{aligned} \pi_J : H(m, 2) &\longrightarrow H(J, 2) \\ (\alpha_1, \dots, \alpha_m) &\longmapsto (\alpha_{i_1}, \dots, \alpha_{i_k}) \end{aligned}$$

Note that we can identify  $H(J, 2)$  with  $H(|J|, 2)$ . We define the *projected code of  $C$  with respect to  $J$*  to be the set  $\pi_J(C) = \{\pi_J(\alpha) : \alpha \in C\}$ . It follows that if  $J = M \setminus \{p\}$  then  $\pi_J(C) = C^{(p)}$ . We have an induced action of  $\text{Aut}(\Gamma)_J = \{g\sigma \in \text{Aut}(\Gamma) : J^\sigma = J\}$  on  $H(J, 2)$  as follows: for  $x \in \text{Aut}(\Gamma)_J$ , we define  $\chi(x) : H(J, 2) \rightarrow H(J, 2)$  by  $\pi_J(\alpha) \mapsto \pi_J(\alpha^x)$ , and obtain  $\chi(\text{Aut}(\Gamma)_J) \leq \text{Aut}(H(J, 2))$  with  $\ker \chi = \{(g_1, \dots, g_m)\sigma \in \text{Aut}(\Gamma)_J : j^\sigma = j \text{ and } g_j = 1 \text{ for } j \in J\}$ .

Let  $\mathcal{D} = (\mathcal{P}, \mathcal{B})$  where  $\mathcal{P}$  is a set of points of cardinality  $m$ , and  $\mathcal{B}$  is a set of  $k$ -subsets of  $\mathcal{P}$  called blocks. Then  $\mathcal{D}$  is a  $t - (m, k, \lambda)$  design if every  $t$ -subset of  $\mathcal{P}$  is contained in exactly  $\lambda$  blocks of  $\mathcal{B}$ . We let  $b$  denote the number of blocks in  $\mathcal{D}$ . If  $\mathcal{D}$  is a  $t$ -design, then it is also an  $i - (m, k, \lambda_i)$  design for  $0 \leq i \leq t - 1$  [7, Corollary 1.6] where

$$(2.3) \quad \lambda_i \binom{k-i}{t-i} = \lambda \binom{m-i}{t-i}.$$

Using this fact we deduce that

$$(2.4) \quad \binom{m}{i} \lambda_i = b \binom{k}{i}.$$

An *automorphism of  $\mathcal{D}$*  is a permutation of  $\mathcal{P}$  that preserves  $\mathcal{B}$ , and we let  $\text{Aut}(\mathcal{D})$  denote the group of automorphisms of  $\mathcal{D}$ . For further concepts and definitions about  $t$ -designs see [7].

**Remark 2.4.** Two designs that appear in this paper are  $\mathcal{D}$ , a  $2 - (11, 5, 2)$  design, and  $\mathcal{E}$ , a  $3 - (12, 6, 2)$  design. Todd proved that  $\mathcal{D}$  is the unique design with these parameters up to isomorphism, and that  $\text{Aut}(\mathcal{D}) \cong \text{PSL}(2, 11)$  [23]. Using this we can prove that  $\mathcal{E}$  is unique up to isomorphism (see [10, Ch. 2], for example). Furthermore, it is known that  $\text{Aut}(\mathcal{E}) \cong M_{11}$ , acting 3-transitively on 12 points [15].

For  $\alpha, \beta \in V(\Gamma)$ , we say  $\alpha$  is *covered by  $\beta$*  if for each non-zero component  $\alpha_i$  of  $\alpha$ , we have  $\alpha_i = \beta_i$ . Let  $\mathcal{D}$  be a set of vertices of weight  $k$  in  $V(\Gamma)$  and  $t \leq k$ . We say  $\mathcal{D}$  is a *2-ary  $t - (m, k, \lambda)$  design* if every vertex of weight  $t$  in  $V(\Gamma)$  is covered by exactly  $\lambda$  vertices of  $\mathcal{D}$ . This definition coincides with the usual definition of a  $t$ -design, in the sense that the set of blocks of the  $t$ -design is the set of supports of vertices in  $\mathcal{D}$ , and as such we simply refer to 2-ary designs as  $t$ -designs. It is known that, for a completely regular code  $C$  in  $H(m, 2)$  with zero codeword and minimum distance  $\delta$ , the set  $C(k)$  of codewords of weight  $k$  forms a  $t - (m, k, \lambda)$  design for some  $\lambda$  with  $t = \lfloor \frac{\delta}{2} \rfloor$  [13].

### 3. HADAMARD CODES AND THEIR AUTOMORPHISM GROUPS

A *Hadamard matrix* of order  $m$  is an  $m \times m$  matrix  $H$  with entries  $\pm 1$  satisfying  $HH^T = mI$ . We denote the  $i$ th row of a Hadamard matrix  $H$  by  $r_i$ . A consequence of the definition of  $H$  is that  $(r_i \cdot r_j) = m\delta_{ij}$ , where  $(-\cdot-)$  denotes the standard dot product and  $\delta_{ij}$  is the Kronecker delta function. Any two Hadamard matrices  $H_1, H_2$  of order  $m$  are said to be *equivalent* if there exist  $m \times m$  monomial matrices  $P, U$ , with nonzero entries  $\pm 1$ , such that  $H_1 = PH_2U$ . Let  $\text{Mon}_m(\pm 1)$  denote the group of

$m \times m$  monomial matrices with nonzero entries  $\pm 1$ . For  $P, U \in \text{Mon}_m(\pm 1)$ , we let  $\varphi_{P,U}$  denote the map  $H \mapsto PHU$ , and call  $\varphi_{P,U}$  an *automorphism of  $H$*  if  $H = PHU$ . We denote the group of automorphisms of  $H$  by  $\text{Aut}(H)$ .

The Hadamard codes were first introduced by Bose and Shrikhande [4], and studied further in [1, 13]. Our treatment follows that in [4, 13]. Let  $V_m(\pm 1) = \{(a_1, \dots, a_m) : a_i = \pm 1\}$  and define the following bijection:

$$\begin{aligned} \kappa : V_m(\pm 1) &\longrightarrow H(m, 2) \\ (a_1, \dots, a_m) &\longmapsto (\alpha_1, \dots, \alpha_m) \end{aligned} \quad \text{where } \alpha_i = \begin{cases} 1 & \text{if } a_i = -1 \\ 0 & \text{if } a_i = 1. \end{cases}$$

The *Hadamard code* generated by a Hadamard matrix  $H$  of order  $m$  is defined as

$$C(H) := \{\kappa(r) : r \text{ is a row of } H \text{ or } -H\}.$$

Bose and Shrikhande showed that  $C(H)$  is an  $(m, 2m, \frac{1}{2}m)$  code. Also, we note that since  $\kappa(-r) \in C(H)$  for all  $\kappa(r) \in C(H)$ , it follows that  $C(H)$  is antipodal. Let  $\tau$  be the monomorphism

$$(3.1) \quad \begin{aligned} \tau : \text{Aut}(H) &\longrightarrow \text{Mon}_m(\pm 1) \\ \varphi_{P,U} &\longmapsto U \end{aligned}$$

Any  $U \in \text{Mon}_m(\pm 1)$  can be described uniquely as a product of a diagonal matrix  $U_D = \text{Diag}(u_1, \dots, u_m)$ , with  $u_i = \pm 1$ , followed by a permutation matrix  $U_\sigma = (u_{ij})$ , where  $\sigma \in S_m$  and  $u_{ij} = 0$  if  $j \neq i^\sigma$ ,  $u_{i,i^\sigma} = 1$ . If  $\Gamma = H(m, 2)$  it follows that  $\text{Mon}_m(\pm 1) \cong \text{Aut}(\Gamma)$  via the isomorphism

$$(3.2) \quad \begin{aligned} \theta : \text{Mon}_m(\pm 1) &\longrightarrow \text{Aut}(\Gamma) \\ U = U_D U_\sigma &\longmapsto (\theta^*(u_1), \dots, \theta^*(u_m))\sigma, \end{aligned}$$

where  $\theta^*$  is the unique isomorphism from the multiplicative group  $Z = \{1, -1\}$  to  $S_2$ . With respect to  $\theta$  and  $\kappa$ , the action of  $\text{Mon}_m(\pm 1)$  on  $V_m(\pm 1)$  is permutationally isomorphic to  $\text{Aut}(\Gamma)$  acting on  $V(\Gamma)$ . That is

$$(3.3) \quad \kappa(vU) = \kappa(v)^{U^\theta}, \quad \forall U \in \text{Mon}_m(\pm 1), \forall v \in V_m(\pm 1).$$

**Proposition 3.1.** *Let  $H$  be a Hadamard matrix of order  $m$ . Then  $\tau\theta$  is an isomorphism from  $\text{Aut}(H)$  to  $\text{Aut}(C(H))$ , where  $\tau, \theta$  are as in (3.1), (3.2) respectively.*

*Proof.* Let  $P = P_D P_\sigma, U \in \text{Mon}_m(\pm 1)$  and  $\overline{H} := PHU$ . Let  $\alpha \in C(H)$ , so  $\alpha = \kappa(\lambda r_i)$  for some row  $r_i$  of  $H$  and  $\lambda = \pm 1$ . By (3.3), it holds that  $\kappa(\lambda r_i)^{U^\theta} = \kappa(\lambda r_i U)$ . Since  $P^{-1}\overline{H} = HU$ , we deduce that  $\lambda r_i U = \bar{\lambda} \bar{r}_{i^\sigma}$ , where  $\bar{r}_{i^\sigma}$  is the  $i^\sigma$ -th row of  $\overline{H}$  and  $\bar{\lambda} = \pm 1$ . Thus  $\alpha^{U^\theta} = \kappa(\bar{\lambda} \bar{r}_{i^\sigma}) \in C(\overline{H})$ . As  $C(H)$  and  $C(\overline{H})$  have the same cardinality, it follows that  $C(H)^{U^\theta} = C(\overline{H}) = C(PHU)$ . In particular, equivalent Hadamard matrices generate equivalent codes, and if  $\varphi_{P,U} \in \text{Aut}(H)$  then  $U^\theta \in \text{Aut}(C)$ . That is,  $(\text{Aut}(H))\tau\theta \leq \text{Aut}(C(H))$ .

Let  $x \in \text{Aut}(C(H))$  and set  $U := x\theta^{-1} \in \text{Mon}_m(\pm 1)$ . Let  $P := HU^{-1}H^{-1}$ , so  $PHU = H$ , and since  $H^{-1} = \frac{1}{m}H^T$ , it follows that  $P_{ik} = \frac{1}{m}(r_i U^{-1} \cdot r_k)$ . We claim that  $P$  is a monomial matrix, and so  $\varphi_{P,U} \in \text{Aut}(H)$  and  $(\varphi_{P,U})\tau\theta = x$ . Since  $U^\theta \in \text{Aut}(C(H))$ , we deduce that  $\kappa(r_i U^{-1}) = \kappa(r_i)^{U^{-1\theta}} \in C(H)$  for each  $i$ . In particular, there exist  $r_{j_i}, \lambda_i = \pm 1$  such that  $r_i U^{-1} = \lambda_i r_{j_i}$  for each  $i$ . As  $C(H)$  is antipodal, it follows that  $\text{Aut}(C(H))$  acts on the set of pairs of complementary

codewords in  $C(H)$ , from which we deduce that  $U^{-1}$  maps  $\{r_1, \dots, r_m\}$  to a set of pairwise orthogonal vectors. Thus, for each  $i$ , there exists a unique  $k$  such that  $(r_{j_i} \cdot r_k) \neq 0$ , and because these are rows of a Hadamard matrix it follows that  $(r_{j_i} \cdot r_k) = m\delta_{j_i k}$ . Thus  $P_{ik} = \lambda_i \delta_{j_i k}$ , so  $P \in \text{Mon}_m(\pm 1)$  and the claim holds.  $\square$

#### 4. THE HADAMARD 12 AND PUNCTURED HADAMARD 12 CODES

In this section we consider Hadamard codes generated by Hadamard matrices of order 12. It is known that a Hadamard matrix of order 12 is unique up to equivalence [14], and we saw in the proof of Proposition 3.1 that equivalent Hadamard matrices generate equivalent Hadamard codes. Therefore we can choose a normalised Hadamard matrix  $H_{12}$  of order 12, namely one in which the first row and first column have all entries equal to 1. We call the Hadamard code  $C(H_{12})$  the *Hadamard 12 code*. Throughout this section  $C$  denotes the Hadamard 12 code, and  $C^{(1)}$  denotes the *punctured Hadamard 12 code* generated by deleting the first entry of each codeword of  $C$ . By [4],  $C$  is a  $(12, 24, 6)$  code and  $C^{(1)}$  is an  $(11, 24, 5)$  code. Van Lint [16] showed that  $C^{(1)}$  is uniformly packed in the sense of [13] with covering radius  $\rho^{(1)} = 3$ . Thus, by [13, Cor 12.2],  $C^{(1)}$  is completely regular. Because  $H_{12}$  is normalised, it follows that the extended code of  $C^{(1)}$  with the parity check bit placed at the front of each codeword is equal to  $C$ . A result by Bassalygo and Zinoviev [1] therefore implies that  $C$  is uniformly packed (in the wide sense), and so by Lemma 2.3,  $C$  is completely regular with covering radius  $\rho = 4$ .

The code  $C$  consists of the zero vertex, the all 1 vertex and 22 vertices of weight 6. As  $C$  is completely regular, it follows from [13] that  $C(6)$ , the set of codewords in  $C$  of weight 6, forms a  $3 - (12, 6, 2)$  design. In this design, the number of blocks that contain the first entry is  $r = 11$ . Thus  $C^{(1)}$  consists of 11 codewords of weight 5 and their complements, as well as the zero and all 1 vertices. It follows from [4] (or from the fact  $C^{(1)}$  is completely regular) that  $C^{(1)}(5)$  forms a  $2 - (11, 5, 2)$  design. Hall [14] showed that  $\text{Aut}(H_{12})$  is the (non-split) double cover  $2M_{12}$ , and therefore, by Proposition 3.1,  $\text{Aut}(C) \cong 2M_{12}$ .

**Proposition 4.1.** *The Hadamard 12 code  $C$  is  $\text{Aut}(C)$ -completely transitive.*

*Proof.* Let  $\mathcal{E}$  be the  $3 - (12, 6, 2)$  design with block set  $C(6)$  and  $\alpha$  be the zero codeword. Any automorphism  $\sigma \in \text{Aut}(C)_\alpha = \text{Aut}(C) \cap L$  naturally induces an automorphism of  $\mathcal{E}$ , and similarly the converse holds. Thus  $\text{Aut}(C)_\alpha \cong \text{Aut}(\mathcal{E}) \cong M_{11}$  acting 3-transitively on 12 points [15], which is a subgroup of index 24 in  $\text{Aut}(C) \cong 2M_{12}$ . Hence  $\text{Aut}(C)$  acts transitively on  $C$ . Thus, because  $\text{Aut}(C)_\alpha$  acts transitively on  $\Gamma_i(\alpha)$  for  $i = 1, 2, 3$ , and since  $\delta = 6$ , it follows that  $\text{Aut}(C)$  acts transitively on  $C_i$  for  $i = 1, 2, 3$ .

Let  $M = \{1, \dots, 12\}$  and  $\tilde{\nu} \in \Gamma_4(\alpha)$ . Then  $\tilde{\nu}$  is adjacent to a weight 3 vertex, which because  $\delta = 6$  is an element of  $C_3$ . Thus  $\tilde{\nu} \in C_2 \cup C_3 \cup C_4$ . Suppose  $\tilde{\nu} \in C_3$ . Then there exists a codeword  $\beta$  such that  $d(\beta, \tilde{\nu}) = 3$ . Because  $\tilde{\nu}$  has weight 4 we deduce that  $\beta$  has odd weight. However,  $C$  consists of codewords of only even weight. Therefore  $\tilde{\nu} \in C_2 \cup C_4$ . For any codeword  $\beta$  of weight 6, there exist  $\binom{6}{4}$  vertices of weight 4 that are at distance 2 from  $\beta$ . Thus  $\Gamma_4(\alpha) \cap C_2 \neq \emptyset$ . Additionally, because  $\text{Aut}(C)$  acts transitively on  $C$  and leaves the distance partition invariant it follows that  $\Gamma_4(\alpha) \cap C_4 \neq \emptyset$ . Thus, as  $\text{Aut}(C)_\alpha$  fixes  $\Gamma_4(\alpha)$  setwise, we deduce that  $\text{Aut}(C)_\alpha$  has at least two orbits on  $\Gamma_4(\alpha)$ , and so it

also has at least two orbits in its induced action on the set of 4-subsets of  $M$ , which we denote by  $M^{\{4\}}$ . The inner product of the permutation characters for the actions of  $M_{12}$  on  $M^{\{4\}}$  and on the right cosets of  $M_{11}$  is 2 (see [8, p. 33]), and is equal to the number of orbits of  $\text{Aut}(C)_\alpha \cong M_{11}$  on  $M^{\{4\}}$ . Thus  $\text{Aut}(C)_\alpha$  has exactly two orbits on  $\Gamma_4(\alpha)$ , and so acts transitively on  $\Gamma_4(\alpha) \cap C_4$ . Therefore Lemma 2.2 implies that  $\text{Aut}(C)$  acts transitively on  $C_4$ .  $\square$

**Proposition 4.2.** *The punctured Hadamard 12 code  $C^{(1)}$  is  $\text{Aut}(C^{(1)})$ -completely transitive.*

*Proof.* Let  $\Gamma = H(12, 2)$  and  $\Gamma' = H(11, 2)$ . Recall from Section 2 that we can describe  $C^{(1)}$  as the projected code  $\pi_J(C)$  where  $J = M \setminus \{1\}$ . Further recall the homomorphism  $\chi$  from  $\text{Aut}(\Gamma)_1$  onto  $\text{Aut}(H(J, 2)) \cong \text{Aut}(\Gamma')$ . It is straight forward to check that  $\chi(\text{Aut}(C)) \cap \ker \chi = 1$  and that  $\chi(\text{Aut}(C)_1) \leq \text{Aut}(C^{(1)})$ . Let  $\alpha \in C$  be the zero codeword. Since  $\text{Aut}(C)_\alpha \cong M_{11}$  acts transitively on  $M$ , it follows that  $\text{Aut}(C)_1$  is transitive on  $C$ , which implies that  $\chi(\text{Aut}(C)_1)$  is transitive on  $C^{(1)}$ .

Let  $\alpha' \in C^{(1)}$  be the zero codeword. Then  $\text{Aut}(C^{(1)})_{\alpha'}$  contains  $\chi(\text{Aut}(C)_1 \cap \text{Aut}(C)_\alpha) \cong \text{PSL}(2, 11)$  acting 2-transitively on  $J$ . Since  $C^{(1)}$  has minimum distance  $\delta = 5$ , arguing as in the proof of Proposition 4.1,  $\chi(\text{Aut}(C)_1)$  is transitive on  $C_i^{(1)}$  for  $i = 1, 2$ ; each weight 3 vertex in  $\Gamma'$  lies in  $C_2^{(1)} \cup C_3^{(1)}$ ; and  $\Gamma'_3(\alpha') \cap C_i^{(1)}$  is non-empty for  $i = 2, 3$ . Thus  $\text{Aut}(C^{(1)})_{\alpha'}$  has at least two orbits on  $\Gamma'_3(\alpha')$ , and hence at least two orbits in its action on  $J^{\{3\}}$ . Then inner product of the permutation characters for the actions of  $M_{11}$  on  $J^{\{3\}}$  and on the right cosets of  $\text{PSL}(2, 11)$  is 2 (see [8, p. 18]). Hence  $\text{Aut}(C^{(1)})_{\alpha'}$  has two orbits on  $\Gamma'_3(\alpha')$ , and so acts transitively on  $\Gamma'_3(\alpha') \cap C_3^{(1)}$ . Thus Lemma 2.2 implies that  $\text{Aut}(C^{(1)})$  acts transitively on  $C_3^{(1)}$ .  $\square$

## 5. PROOF OF THEOREM 1.1

Let  $C$  be a completely regular code in  $H(m, 2)$  with minimum distance  $\delta$  for  $(m, \delta) = (12, 6)$  or  $(11, 5)$ . Also, let  $A(m, \delta)$  denote the maximum number of codewords in any binary code of length  $m$  with minimum distance  $\delta$ . By [17, App. A, Fig. 1],  $A(11, 5) = 24$ , and by [17, p. 42],  $A(12, 6) = A(11, 5) = 24$ . Hence  $|C| \leq 24$ .

As automorphisms of the Hamming graph preserve the property of complete regularity, by replacing  $C$  with an equivalent code if necessary, we may assume the zero vertex,  $\alpha$ , is a codeword in  $C$ . Since  $C$  is completely regular with minimum distance  $\delta$ , it follows that  $C(\delta) = \Gamma_\delta(\alpha) \cap C \neq \emptyset$ . Thus  $C(\delta)$  forms a  $t - (m, \delta, \lambda)$  design for some  $\lambda$ , where  $t = \lfloor \frac{m}{2} \rfloor$ . In both cases  $((m, \delta) = (12, 6)$  or  $(11, 5))$ , we deduce from (2.3) and (2.4) that 2 divides  $\lambda$ . Consider the codewords of weight  $\delta$  whose support contains  $\{1, 2, \dots, t\}$ . Because  $C$  has minimum distance  $\delta$ , it follows that the intersection of the supports of any two of these codewords is  $\{1, \dots, t\}$ . Consequently, a simple counting argument gives  $\lambda \leq (m - t)/(\delta - t)$ . In both cases we deduce that  $\lambda \leq 3$ , and so  $\lambda = 2$ .

**Case  $(m, \delta) = (12, 6)$ :** As  $C(6)$  forms a  $3 - (12, 6, 2)$  design, it follows that  $|C(6)| = 22$ . This design is the extension of a symmetric  $2 - (11, 5, 2)$  design, and so, by [7, p.11], we deduce that for all  $\beta \in C(6)$ , the complement  $\beta^c \in C(6)$ . Thus, because  $C$  is completely regular, it follows that  $C$  is antipodal, so  $\alpha^c \in C$  and  $|C| \geq 1 + 22 + 1 = 24$ . As  $|C| \leq 24$ , we conclude that  $C$  consists exactly of  $\alpha, \alpha^c$  and 22 codewords of weight 6 that form a  $3 - (12, 6, 2)$  design. The same holds for the Hadamard 12 code, and

by Remark 2.4, this design is unique up to isomorphism. Thus there exists an automorphism  $\sigma \in L$  (the top group of  $\text{Aut}(\Gamma)$ ) such that  $C^\sigma$  is the Hadamard 12 code. This proves Theorem 1.1 (a).

**Case  $(m, \delta) = (11, 5)$ :** As  $C(5)$  forms a  $2 - (11, 5, 2)$  design it follows that  $|C(5)| = 11$ . Let  $\alpha_1, \alpha_2$  be the two codewords in  $C(5)$  whose supports contain  $\{1, 2\}$ . Then  $d(\alpha_1, \alpha_2) = 6$ , and so, because  $C$  is completely regular, it follows that  $C(6)$  forms a  $2 - (11, 6, \mu)$  design for some  $\mu$ . We deduce from (2.3) and (2.4) that 3 divides  $\mu$  and 11 divides  $|C(6)|$ , and so, because  $|C| \leq 24$ ,  $\mu = 3$  and  $|C(6)| = 11$ . Consequently  $|C| = 23$  or 24. If  $|C| = 23$ , then in the distance distribution  $a(C)$ ,  $a_0 = 1$ ,  $a_5 = a_6 = 11$ , and  $a_i = 0$  otherwise. However, if this holds then in the MacWilliams transform of  $a(C)$  (see 2.2),  $a'_2 = \sum_{i=0}^{11} a_i K_2(i) = -55$ , contradicting [16, Lemma 5.3.3]. Thus  $|C| = 24$  and there exists a unique  $i \geq 7$  such that  $a_i = 1$ . Suppose  $i \leq 10$ . Then  $C(i)$  forms a  $2 - (12, i, \mu')$  design, and by Fishers inequality [7, 1.14],  $|C(i)| \geq 11$  which contradicts the fact that  $|C| = 24$ . Thus  $a_{11} = 1$ , which implies that  $C$  is antipodal. Thus  $C$  consists exactly of  $\alpha$ ,  $\alpha^c$ , the 11 codewords of weight 5 that form a  $2 - (11, 5, 2)$  design, and their complements, which form a  $2 - (11, 5, 3)$  design. This is also true for the punctured Hadamard 12 code, and because the  $2 - (11, 5, 2)$  design is unique up to isomorphism [23], there exists  $\sigma \in L$  such that  $C^\sigma$  is the punctured Hadamard 12 code. This proves Theorem 1.1 (b).

By Proposition 4.1 and Proposition 4.2, the Hadamard 12 code and punctured Hadamard 12 code are both completely transitive. Therefore, by [11], any code that is equivalent to either the Hadamard 12 code or punctured Hadamard 12 code is completely transitive. Thus the final statement of Theorem 1.1 follows from parts (a) and (b).

## 6. ACKNOWLEDGMENTS

The authors would like to thank the anonymous reviewers for their valuable comments and suggestions to improve the quality of this paper.

## REFERENCES

- [1] Bassalygo, L.A., Zinov'ev, V.A.: A remark on uniformly packed codes. *Problemy Peredači Informacii* **13**(3), 22–25 (1977)
- [2] Borges, J., Rifà, J., Zinoviev, V.A.: On non-antipodal binary completely regular codes. *Discrete Math.* **308**(16), 3508–3525 (2008)
- [3] Borges, J., Rifà, J., Zinoviev, V.A.: On  $q$ -ary linear completely regular codes with  $\rho = 2$  and antipodal dual. *Adv. Math. Commun.* **4**(4), 567–578 (2010)
- [4] Bose, R.C., Shrikhande, S.S.: A note on a result in the theory of code construction. *Information and Control* **2**, 183–194 (1959)
- [5] Brouwer, A.: On complete regularity of extended codes. *Discrete Mathematics* **117**(13), 271 – 273 (1993)
- [6] Brouwer, A.E., Cohen, A.M., Neumaier, A.: Distance-regular graphs, *Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]*, vol. 18. Springer-Verlag, Berlin (1989)
- [7] Cameron, P.J., van Lint, J.H.: Designs, graphs, codes and their links, *London Mathematical Society Student Texts*, vol. 22. Cambridge University Press, Cambridge (1991)
- [8] Conway, J.H., Curtis, R.T., Norton, S.P., Parker, R.A., Wilson, R.A.: Atlas of finite groups. Oxford University Press, Eynsham (1985). Maximal subgroups and ordinary characters for simple groups, With computational assistance from J. G. Thackray



- [9] Delsarte, P.: An algebraic approach to the association schemes of coding theory. Philips Res. Rep. Suppl. (10), vi+97 (1973)
- [10] Gillespie, N.I.: Neighbour transitivity on codes in Hamming graphs. Ph.D. thesis, The University of Western Australia, Perth, Australia (2011)
- [11] Gillespie, N.I., Praeger, C.E.: From neighbour transitive codes to frequency permutation arrays (2012). ArXiv:1204.2900v1
- [12] Giudici, M., Praeger, C.E.: Completely transitive codes in Hamming graphs. European J. Combin. **20**(7), 647–661 (1999)
- [13] Goethals, J.M., van Tilborg, H.C.A.: Uniformly packed codes. Philips Res. Rep. **30**, 9–36 (1975)
- [14] Hall Jr., M.: Note on the Mathieu group  $M_{12}$ . Arch. Math. (Basel) **13**, 334–340 (1962)
- [15] Hughes, D.R.: On  $t$ -designs and groups. Amer. J. Math. **87**, 761–778 (1965)
- [16] van Lint, J.H.: Recent results on perfect codes and related topics. In: Combinatorics (Proc. NATO Advanced Study Inst., Breukelen, 1974), pp. 158–178. Math. Centre Tracts, No. 55. Math. Centrum, Amsterdam (1974)
- [17] MacWilliams, F.J., Sloane, N.J.A.: The Theory of Error-Correcting Codes. North-Holland Publishing Co., Amsterdam (1977)
- [18] Martin, W.J.: Completely regular codes — a viewpoint and some problems. Proceedings of 2004 Com2MaC Workshop on Distance-Regular Graphs and Finite Geometry pp. 43–56 (2004)
- [19] Neumaier, A.: Completely regular codes. Discrete Math. **106/107**, 353–360 (1992). A collection of contributions in honour of Jack van Lint
- [20] Rifa, J., Zinoviev, V.A.: On a class of binary linear completely transitive codes with arbitrary covering radius. Discrete Math. **309**(16), 5011–5016 (2009)
- [21] Rifa, J., Zinoviev, V.A.: New completely regular  $q$ -ary codes based on Kronecker products. IEEE Trans. Inform. Theory **56**(1), 266–272 (2010)
- [22] Solé, P.: Completely regular codes and completely transitive codes. Discrete Math. **81**(2), 193–201 (1990)
- [23] Todd, J.: A combinatorial problem. J. Math. Phys., Mass. Inst. Techn. **12**, 321–333 (1933)
- [24] Zinov'ev, V.A., Rifa, D.: On new completely regular  $q$ -ary codes. Problemy Peredachi Informatsii **43**(2), 34–51 (2007)

[GILLESPIE AND PRAEGER] CENTRE FOR MATHEMATICS OF SYMMETRY AND COMPUTATION, SCHOOL OF MATHEMATICS AND STATISTICS, THE UNIVERSITY OF WESTERN AUSTRALIA, 35 STIRLING HIGHWAY, CRAWLEY, WESTERN AUSTRALIA 6009

*E-mail address:* neil.gillespie@graduate.uwa.edu.au, cheryl.praeger@uwa.edu.au